

Christopher A. Seeger
Parvin Aminolroaya
SEEGER WEISS LLP
55 Challenger Road
6th Floor
Ridgefield Park, NJ 07660

Jennifer Scullion (pro hac vice forthcoming)
SEEGER WEISS LLP
77 Water Street
8th Floor
New York, NY 10005
(212) 584-0700

Attorneys for Plaintiffs
(Additional Counsel on the Signature Page)

**UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY**

MARK MEISEL, ZAKARIA HAQUE, ROBERT
OSWALD, LORI WEINRIB, ROBERT CORWIN,
and CINDY FARBER, individually and on behalf of
all those similarly situated,

Plaintiffs,

v.

AMERICAN MEDICAL COLLECTION AGENCY,
INC., OPTUM360 SERVICES, INC., QUEST
DIAGNOSTICS INCORPORATED, and DOES 1-10,

Defendants.

Civil Action No.

**COMPLAINT and
DEMAND FOR JURY TRIAL**

Plaintiffs Mark Meisel, Zakaria Haque, Robert Oswald, Lori Weinrib and Robert Corwin (“Plaintiffs”), individually and on behalf of all others similarly situated, through the undersigned counsel, hereby alleges the following, against Defendants American Medical Collection Agency, Inc. (“AMCA”), Optum360 Services, Inc. (“Optum360”), and Quest Diagnostics Incorporated (“Quest”) (collectively, “Defendants”). Based upon personal

knowledge, information, belief, and investigation of counsel, Plaintiffs specifically allege as follows:

SUMMARY OF THE CASE

1. Plaintiffs bring this class action on behalf of a nationwide class and a California Sub-Class (together, the “Classes”) against Defendants because of their failure to protect the confidential information of millions of patients—including financial information (*e.g.*, credit card numbers and bank account information), medical information, personal information (*e.g.*, Social Security Numbers), and/or other protected health information as defined by the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) (collectively, their “Sensitive Information”). Defendants’ wrongful disclosure has harmed Plaintiffs and the Classes, believed to include thousands of individuals.

JURISDICTION AND VENUE

2. This Court has subject matter jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d) in that: (1) this is a class action involving more than 1,000 class members; (2) minimal diversity is present as Plaintiffs are citizens of New Jersey, Connecticut and New York (and the proposed class members are from various states) while Defendants are citizens of New York, Minnesota, and New Jersey; and (3) the amount in controversy exceeds the sum of \$5,000,000, exclusive of interest and costs.

3. This Court has personal jurisdiction over Defendants because Defendants do business in and throughout New Jersey, and the wrongful acts alleged in this Complaint were committed in New Jersey, among other venues.

4. Venue is proper in this District pursuant to: (1) 28 U.S.C. § 1391(b)(2) in that a substantial part of the events or omissions giving rise to Plaintiffs’ claims occurred in this

District, and 28 U.S.C. § 1391(d) because the transactions giving rise to the claims occurred in Secaucus, New Jersey; and (2) 28 U.S.C. § 1391(b)(3) in that Defendants are subject to personal jurisdiction in this District.

PARTIES

5. Plaintiff Mark Meisel is an individual residing in Haworth, New Jersey, who has been a patient of Quest and whose Sensitive Information, on information and belief, was compromised in the Data Breach described herein.

6. Plaintiff Zakaria Haque is an individual residing in Milford, Connecticut, who has been a patient of Quest and whose Sensitive Information, on information and belief, was compromised in the Data Breach described herein.

7. Plaintiff Robert Oswald is an individual residing in Mahopac, New York, who has been a patient of Quest and whose Sensitive Information, on information and belief, was compromised in the Data Breach described herein.

8. Plaintiff Lori Weinrib is an individual residing in New City, New York, who has been a patient of Quest and whose Sensitive Information, on information and belief, was compromised in the Data Breach described herein.

9. Plaintiff Robert Corwin is an individual residing in New City, New York, who has been a patient at a Quest facility in Florida, and whose Sensitive Information, on information and belief, was compromised in the Data Breach described herein.

10. Plaintiff Cindy Farber is an individual residing in Naples, Florida, who has been a patient of Quest facility, and whose Sensitive Information, on information and belief, was compromised in the Data Breach described herein.

11. Defendant American Medical Collection Agency, Inc. (“AMCA”) is a New York corporation with its principal place of business in Elmsford, New York.

12. Defendant Quest Diagnostics Incorporated (“Quest”) is a Delaware corporation with its principal place of business in Secaucus, New Jersey.

13. Based on information and belief, Defendant Optum360 Services, Inc. (“Optum360”) is a Delaware corporation with its principal place of business in Eden Prairie, Minnesota.

FACTUAL BACKGROUND

14. Quest is the world’s leading provider of medical diagnostic testing services. It performs medical tests that aid in the diagnosis or detection of diseases, and that measure the progress of or recovery from a disease.

15. On June 3, 2019, Quest publicly admitted in a filing with the Securities and Exchange Commission (“SEC”) that: “On May 14, 2019, American Medical Collection Agency (AMCA), a billing collections vendor, notified Quest . . . and Optum360 LLC, [Quest’s] revenue cycle management provider,” of a massive data breach compromising the Sensitive Information of 11.9 million Quest patients, and most likely others (the “Data Breach”). Quest Form 8-K, June 3, 2019.

16. Quest’s SEC filing disclosed that, “between August 1, 2018 and March 30, 2019 an unauthorized user had access to AMCA’s system that contained information that AMCA had received from various entities, including Quest Diagnostics, and information that AMCA collected itself[,] . . . include[ing] financial information (e.g., credit card numbers and bank account information), medical information[,] and other personal information (e.g., Social Security Numbers).” *Id.*

17. Quest apparently allowed hackers to access Plaintiffs' and other Class Members' Sensitive Information for some seven months and did nothing to let the victims know about the Data Breach for nearly a year after it began.

18. Although Quest knew of the Data Breach at least as of May 14, 2019, and although AMCA knew of it even earlier, neither took any steps to notify patients whose information was affected until June 3, 2019, at which point Quest only did so through an SEC filing.

19. Defendants had obligations created by HIPAA, arising from promises made to patients like Plaintiffs and other Class Members, and based on industry standards, to keep the compromised Sensitive Information confidential and to protect it from unauthorized disclosures. Class Members provided their Sensitive Information to Quest with the understanding that Quest and any business partners to whom Quest disclosed the Sensitive Information would comply with their obligations to keep such information confidential and secure from unauthorized disclosures.

20. Indeed, Quest promises patients that it will keep their Sensitive Information confidential, assuring patients that it is "committed to protecting the privacy of your identifiable health information." Quest Diagnostics, *Notice of Privacy Practices*, <http://questdiagnostics.com/home/privacy-policy/notice-privacy-practices.html> (last visited June 3, 2019).

21. In its Notice of Privacy Practices, Quest acknowledges that it is subject to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). *Id.*

22. Quest informs patients: "We may provide your PHI [(Private Health Information)] to other companies or individuals that need the information to provide services to us. These other

entities, known as ‘business associates,’ are required to maintain the privacy and security of PHI.” *Id.*

23. Defendants’ data security obligations and promises were particularly important given the substantial increase in data breaches — particularly those in the healthcare industry — preceding August 2018, which were widely known to the public and to anyone in Defendants’ industries.

24. Defendants’ security failures demonstrate that they failed to honor their duties and promises by not:

- a. Maintaining an adequate data security system to reduce the risk of data breaches and cyber-attacks;
- b. Adequately protecting Plaintiffs’ and the Classes’ Sensitive Information;
- c. Ensuring the confidentiality and integrity of electronic protected health information they created, received, maintained, or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);
- d. Implementing technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights, in violation of 45 C.F.R. § 164.312(a)(1);
- e. Implementing policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 C.F.R. § 164.308(a)(1)(i);
- f. Implementing procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

- g. Protecting against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information, in violation of 45 C.F.R. § 164.306(a)(2);
- h. Protecting against reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 C.F.R. § 164.306(a)(3);
- i. Ensuring compliance with the electronically protected health information security standard rules by their workforces, in violation of 45 C.F.R. § 164.306(a)(4);
and/or
- j. Training all members of their workforces effectively on the policies and procedures with respect to protected health information as necessary and appropriate for the members of their workforces to carry out their functions and to maintain security of protected health information, in violation of 45 C.F.R. § 164.530(b).

It is Well-Established That Data Breaches Lead to Identity Theft

25. Plaintiffs and other Class Members have been injured by the disclosure of their Sensitive Information in the Data Breach.

26. The United States Government Accountability Office noted in a June 2007 report on Data Breaches (“GAO Report”) that identity thieves use identifying data such as Social Security Numbers to open financial accounts, receive government benefits and incur charges and credit in

a person's name.¹ As the GAO Report states, this type of identity theft is the most harmful because it often takes some time for the victim to become aware of the theft, and the theft can impact the victim's credit rating adversely.

27. In addition, the GAO Report states that victims of identity theft will face "substantial costs and inconveniences repairing damage to their credit records" and their "good name."²

28. Identity theft victims frequently are required to spend many hours and large amounts of money repairing the impact to their credit. Identity thieves use stolen personal information such as social security numbers ("SSNs") for a variety of crimes, including credit card fraud, phone or utilities fraud, and/or bank/finance fraud.

29. There may be a time lag between when Sensitive Information is stolen and when it is used. According to the GAO Report:

[L]aw enforcement officials told us that in some cases, *stolen data may be held for up to a year or more before being used to commit identity theft*. Further, once stolen data have been sold or posted on the Web, *fraudulent use of that information may continue for years*. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.³

30. With access to an individual's Sensitive Information, criminals can do more than just empty a victim's bank account—they can also commit all manner of fraud, including: obtaining a driver's license or official identification card in the victim's name but with the thief's picture; using the victim's name and SSN to obtain government benefits; or, filing a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the

¹ See *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent Is Unknown* (June 2007), United States Government Accountability Office, available at <<https://www.gao.gov/new.items/d07737.pdf>> (last visited June 4, 2019).

² *Id.* at 2, 9

³ *Id.* at 29 (emphasis supplied).

victim's SSN, rent a house, or receive medical services in the victim's name. Identity thieves may even give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.⁴

31. Sensitive Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the “cyber black-market” for years. As a result of recent large-scale data breaches, identity thieves and cyber criminals have openly posted stolen credit card numbers, SSNs, and other Sensitive Information directly on various Internet websites making the information publicly available.

32. A study by Experian found that the “average total cost” of medical identity theft is “about \$20,000” per incident, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.⁵

33. Indeed, data breaches and identity theft have a crippling effect on individuals and detrimentally impact the entire economy as a whole. Medical databases are especially valuable to identity thieves. According to a 2012 Nationwide Insurance report, “[a] stolen medical identity has a \$50 street value – whereas a stolen social security number, on the other hand, only sells for \$1.”⁶ In fact, the medical industry has experienced disproportionately higher instances of computer theft than any other industry.

⁴ See Federal Trade Commission, *Warning Signs of Identify Theft*, available at <https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft> (last visited June 4, 2019).

⁵ See Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET, (Mar. 3, 2010) <https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims> (last visited June 4, 2019).

⁶ See Study; *Few Aware of Medical Identity Theft Risk*, Claims Journal, <http://www.claimsjournal.com/news/national/2012/06/14/208510.htm> (last visited June 4, 2019).

CLASS ALLEGATIONS

34. In accordance with Federal Rules of Civil Procedure 23(b)(2) and (b)(3), Plaintiffs bring this case as a class action on behalf of a Nationwide Class, and a California Sub-Class, defined as follows:

Nationwide Class: All persons in the United States whose Sensitive Information was maintained on the AMCA systems that were compromised as a result of the breach announced by Quest on or around June 3, 2019.

California Sub-Class: All persons in the State of California whose Sensitive Information was maintained on the AMCA systems that were compromised as a result of the breach announced by Quest on or around June 3, 2019.

35. The Classes are each so numerous that joinder of all members is impracticable. On information and belief, the Classes each have more than 1,000 members. Moreover, the disposition of the claims of the Classes in a single action will provide substantial benefits to all parties and the Court.

36. There are numerous questions of law and fact common to Plaintiffs and Class Members. These common questions of law and fact include, but are not limited to, the following:

- a. Whether Defendants' data security systems prior to the Data Breach met the requirements of laws including, for instance, HIPAA;
- b. Whether Defendants' data security systems prior to the Data Breach met industry standards;
- c. Whether Plaintiffs' and other Class members' Sensitive Information was compromised in the Data Breach; and
- d. Whether Plaintiffs' and other Class members are entitled to damages as a result of Defendants' conduct.

37. Plaintiffs' claims are typical of the claims of the Classes' claims. Plaintiffs suffered the same injury as Class Members—*i.e.*, upon information and belief, Plaintiffs' Sensitive Information was compromised in the Data Breach.

38. Plaintiffs will fairly and adequately protect the interests of the Classes. Plaintiffs have retained competent and capable attorneys with significant experience in complex and class action litigation, including data breach class actions. Plaintiffs and their counsel are committed to prosecuting this action vigorously on behalf of the Classes and have the financial resources to do so. Neither Plaintiffs nor their counsel have interests that are contrary to or that conflict with those of the proposed Classes.

39. Defendants have engaged in a common course of conduct toward Plaintiffs and other Class Members. The common issues arising from this conduct that affect Plaintiffs and Class Members predominate over any individual issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

40. A class action is the superior method for the fair and efficient adjudication of this controversy. In this regard, the Class Members' interests in individually controlling the prosecution of separate actions is low given the magnitude, burden, and expense of individual prosecutions against large corporations such as Defendants. It is desirable to concentrate this litigation in this forum to avoid burdening the courts with individual lawsuits. Individualized litigation presents a potential for inconsistent or contradictory judgments, and also increases the delay and expense to all parties and the court system presented by the legal and factual issues of this case. By contrast, the class action procedure here will have no management difficulties. Defendants' records and the records available publicly will easily identify the Class Members. The same common documents and testimony will be used to prove Plaintiffs' claims

41. A class action is appropriate under Fed. R. Civ. P. 23(b)(2) because Defendants have acted or refused to act on grounds that apply generally to Class Members, so that final injunctive relief or corresponding declaratory relief is appropriate as to all Class Members.

FIRST COUNT
Negligence
(On behalf of Plaintiffs and the Nationwide Class)

42. Plaintiffs reallege and incorporate by reference all preceding factual allegations.

43. Quest required Plaintiffs and Class Members to submit non-public Personal Information to obtain medical services, which Quest provided to AMCA for billing purposes.

44. By collecting and storing this data, and sharing it and using it for commercial gain, Defendants both had a duty of care to use reasonable means to secure and safeguard this Sensitive Information, to prevent disclosure of the information, and to guard the information from theft.

45. Defendants' duty included a responsibility to implement a process by which they could detect a breach of their security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

46. Defendants also owed a duty of care to Plaintiffs and members of the Classes to provide security consistent with industry standards and the other requirements discussed herein, and to ensure that their systems and networks—and the personnel responsible for them adequately protected their customers' Sensitive Information.

47. Defendants' duty to use reasonable security measures arose as result of the special relationship that existed between Quest and its patients, which is recognized by laws including but not limited to HIPAA. Only Defendants were in a position to ensure that their systems were

sufficient to protect against the harm to Plaintiffs and the members of the Classes from a data breach.

48. Defendants' duty to use reasonable security measures also arose under HIPAA, pursuant to which Defendants are required to "reasonable protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). The confidential data at issue in this case constitutes "protected health information" within the meaning of HIPAA.

49. In addition, Defendants had a duty to use reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

50. Defendants' duty to use reasonable care in protecting confidential data arose not only as a result of the common law and the statutes and regulations described above, but also because they are bound by, and have committed to comply with, industry standards for the protection of confidential Sensitive Information.

51. Defendants breached their common law, statutory and other duties—and thus, were negligent—by failing to use reasonable measures to protect patients' Sensitive Information, and by failing to provide timely notice of the Data Breach.

52. The specific negligent acts and omissions committed by Defendants include, but are not limited to, the following:

- a. failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiffs' and Class members' Sensitive Information;

- b. failing to adequately monitor the security of AMCA's network and systems;
- c. allowing unauthorized access to Plaintiffs' and Class Members' Sensitive Information;
- d. failing to recognize in a timely manner that Plaintiffs' and other Class Members' Sensitive Information had been compromised; and
- e. failing to warn Plaintiffs and other Class Members about the Data Breach in a timely manner so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

53. It was foreseeable that Defendants' failure to use reasonable measures to protect Sensitive Information and to provide timely notice of the Data Breach would result in injury to Plaintiffs and other Class Members. Further, the breach of security, unauthorized access, and resulting injury to Plaintiffs and the members of the Classes were reasonably foreseeable.

54. It was therefore foreseeable that the failure to adequately safeguard Sensitive Information would result in one or more of the following injuries to Plaintiffs and the members of the proposed Class: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the deep web black market; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

55. Accordingly, Plaintiffs, individually and on behalf of all those similarly situated, seek an order declaring that Defendants' conduct constitutes negligence and awarding damages in an amount to be determined at trial.

SECOND COUNT

**Violation of the California Medical Information Act
(On behalf of Plaintiffs and the California Sub-Class)**

56. Plaintiffs reallege and incorporate by reference all preceding factual allegations.

57. Plaintiffs allege additionally and alternatively that California's Confidential Medical Information Act was enacted to protect, among other things, the release of confidential medical information without proper authorization. *See* Confidential Medical Information Act, Cal. Civ. Code §§ 56, *et seq.* ("CMIA"). To that end, the CMIA prohibits entities from negligently disclosing or releasing any person's confidential medical information. *See* Cal. Civ. Code § 56.36 (2013). The CMIA also requires that an entity that "creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information shall do so in a manner that preserves the confidentiality of the information contained therein." Civ. Code § 56.101(a).

58. As described throughout this Complaint, Defendants negligently disclosed and released Plaintiffs' and California Sub-Class Members' Sensitive Information by failing to implement adequate security protocols to prevent unauthorized access to Sensitive Information, failing to maintain an adequate electronic security system to prevent data breaches, failing to employ industry standard and commercially viable measures to mitigate the risks of any data breach, and otherwise failing to comply with HIPAA data security requirements.

59. As a direct and proximate result of Defendants' negligence, they disclosed and released Plaintiffs' and California Sub-Class Members' Sensitive Information to hackers.

60. Accordingly, Plaintiffs seek to recover actual, nominal (including \$1000 nominal damages per disclosure under Cal. Civ. Code § 56.36(b)), and statutory damages (including under § 56.36(c)) where applicable, together with reasonable attorneys' fees and costs.

THIRD COUNT

**Violation of New York General Business Law § 349
(On behalf of Plaintiffs and the Nationwide Class)**

61. Plaintiffs reallege and incorporate by reference all preceding factual allegations.

62. Defendants, while operating in New York, engaged in deceptive acts and practices in the conduct of business, trade and commerce, and the furnishing of services, in violation of N.Y. Gen. Bus. Law § 349(a). This includes but is not limited to the following:

- a. Defendants failed to enact adequate privacy and security measures to protect the Class Members' Sensitive from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach;
- b. Defendants failed to take proper action following known security risks and prior cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Defendants knowingly and fraudulently misrepresented that they would maintain adequate data privacy and security practices and procedures to safeguard the Sensitive Information from unauthorized disclosure, release, data breaches, and theft;
- d. Defendants omitted, suppressed, and concealed the material fact of Defendants' reliance on, and inadequacy of, AMCA's security protections;
- e. Defendants knowingly and fraudulently misrepresented that they would comply with the requirements of relevant federal and state laws pertaining to the privacy

and security of Sensitive Information, including but not limited to duties imposed by HIPAA; and

- f. Defendants failed to disclose the Data Breach to the victims in a timely and accurate manner, in violation of the duties imposed by, *inter alia*, N.Y. Gen Bus. Law § 899-aa(2).

63. As a direct and proximate result of Defendants' practices, Plaintiffs and other Class Members suffered injury and/or damages, including but not limited to time and expenses related to monitoring their financial and medical accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of value of their Sensitive Information.

64. The above unfair and deceptive acts and practices and acts by Defendants were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiffs and other Class Members that they could not reasonably avoid, which outweighed any benefits to consumers or to competition.

65. Defendants knew or should have known that AMCA's computer systems and data security practices were inadequate to safeguard Sensitive Information entrusted to it, and that risk of a data breach or theft was highly likely. Defendants' actions in engaging in the above-referenced unfair practices and deceptive acts were negligent, knowing and willful.

66. Plaintiffs seek relief under N.Y. Gen. Bus. Law § 349(h), including but not limited to actual damages (to be proven at trial), treble damages, statutory damages, injunctive relief, and/or attorney's fees and costs. The amount of such damages is to be determined at trial but will not be less than \$50.00 per violation. *Id.*

67. Plaintiffs and Class Members seek to enjoin such unlawful deceptive acts and practices described above. Each Class Member will be irreparably harmed unless the Court

enjoins Defendants' unlawful, deceptive actions in that Defendants will continue to fail to protect Sensitive Information entrusted to them, as detailed herein.

68. Plaintiffs and Class Members seek declaratory relief, restitution for monies wrongfully obtained, disgorgement of ill-gotten revenues and/or profits, injunctive relief prohibiting Defendant from continuing to disseminate its false and misleading statements, and other relief allowable under N.Y. Gen. Bus. Law § 349.

FOURTH COUNT
Breach of Implied Contract
(On behalf of Plaintiffs and the Nationwide Class)

69. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

70. When Plaintiffs and Class members paid money and provided their Sensitive Information to Defendants in exchange for services, they entered into implied contracts with Defendants pursuant to which Defendants agreed to safeguard and protect such information and to timely and accurately notify them if their data had been breached and compromised.

71. Defendants solicited and invited prospective clients and other consumers to provide their Sensitive Information as part of its regular business practices. These individuals accepted Defendants' offers and provided their Sensitive Information to Defendants. In entering into such implied contracts, Plaintiffs and the Class assumed that Defendants' data security practices and policies were reasonable and consistent with industry standards, and that Defendants would use part of the funds received from Plaintiffs and the Class to pay for adequate and reasonable data security practices.

72. Plaintiffs and the Class would not have provided and entrusted their Sensitive Information to Defendants in the absence of the implied contract between them and Defendants to keep the information secure.

73. Plaintiffs and the Class fully performed their obligations under the implied contracts with Defendants.

74. Defendants breached their implied contracts with Plaintiffs and the Class by failing to safeguard and protect their Sensitive Information and by failing to provide timely and accurate notice that their personal information was compromised as a result of a data breach.

75. As a direct and proximate result of Defendants' breaches of their implied contracts, Plaintiffs and the Class sustained actual losses and damages as described herein.

FIFTH COUNT

Violation of California Unfair Competition Act, Cal. Bus. & Prof. Code § 17200, *et. seq.* (On behalf of Plaintiffs and the California Sub-Class)

76. Plaintiffs reallege and incorporate by reference all preceding factual allegations.

77. Defendants' actions as described herein constitute unfair competition within the meaning of the UCL, insofar as the UCL prohibits "any unlawful, unfair or fraudulent business act or practice."

78. Defendants' conducts as alleged herein constitute unlawful, unfair, and fraudulent business practices in that they deceived the Plaintiffs and California Sub-Class Members into believing their Sensitive Information would be protected by reasonable, industry-standard data security measures.

79. Defendants' conduct constitutes an "unlawful" business practice within the meaning of the UCL because it violates HIPAA, the California Customer Records Act, Cal. Civ. Code §

17980.80 *et seq.*, and other statutes requiring adequate data security to protect Sensitive Information such as that which was compromised in the Data Breach.

80. Defendants' conduct constitutes an "unfair" business practice within the meaning of the UCL because it is immoral, unethical, oppressive, unscrupulous and/or substantially injurious to consumers.

81. As a direct and proximate result of Defendants' wrongful business practices in violation of the UCL, Plaintiffs and California Sub-Class Members have suffered injury in fact and lost money or property as a result of purchasing services from Quest. Plaintiffs and California Sub-Class Members would not have purchased or paid as much for services from Quest had they known the truth about Defendants' data security.

82. Defendants' wrongful business practices constitute a continuing course of conduct of unfair competition since Defendants continue to employ deficient data security measures.

83. Pursuant to Cal. Bus. & Prof. Code § 17203, Plaintiffs and the California Sub-Class Members seek an order of this Court enjoining Defendants from continuing to engage in unlawful, unfair, and fraudulent business practices and any other act prohibited by law, including those set forth in this Complaint. Plaintiffs and the California Sub-Class Members also seek an order requiring Defendants to make full restitution of all moneys it wrongfully obtained from the Plaintiffs and the Class.

84. Pursuant to Cal. Bus. & Prof. Code § 17203, Plaintiffs and California Sub-Class Members seek an injunction enjoining Defendant from continuing to employ deficient data security.

SIXTH COUNT

**Violation of the California Customer Records Act, Cal. Civil Code §§ 1798.81.5 & 1798.82
(On behalf of Plaintiffs and the California Sub-Class)**

85. Plaintiffs reallege and incorporate by reference each of the allegations set forth above.

86. “[T]o ensure that personal information about California residents is protected,” the California legislature enacted Civil Code section 1798.81.5, which requires that any business that “owns or licenses personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.”

87. The Sensitive Information taken in the Data Breach fits within the definition of “Personal information” in Civil Code section 1798.80.

88. Plaintiffs and other Class Members provided their personal information to Defendants in order to get medical diagnoses. These patients qualify as “Customer[s]” as defined in Civil Code section 1798.80.

89. By failing to implement reasonable measures to protect the Sensitive Information in their possession, Defendants violated Civil Code section 1798.81.5.

90. In addition, by failing to promptly notify all who were affected by the Data Breach that their Sensitive Information had been acquired (or was reasonably believed to have been acquired) by hackers, Defendants violated Civil Code Section 1798.82.

91. As a direct or proximate result of Defendants’ violations of Civil Code Sections 1798.81, 1798.81.5, and 1798.82, Plaintiffs and Class Members were (and continue to be)

injured and have suffered (and will continue to suffer) the damages described in this Class Action Complaint.

92. Defendants' violations of Civil Code Sections 1798.81, 1798.81.5, and 1798.82 were, at a minimum, reckless.

93. In addition, by violating Civil Code Sections 1798.81, 1798.81.5, and 1798.82, Defendants "may be enjoined" under Civil Code Section 1798.84(e).

94. Defendants' violations of Civil Code Section 1798.81.5 and 1798.82 also constitute an unlawful acts or practices under California's Unfair Competition Law (UCL), Cal. Bus. & Prof. Code § 17200 et seq., which affords the Court discretion to enter whatever orders may be necessary to prevent future unlawful acts or practices.

95. Plaintiffs accordingly request that the Court enter an injunction requiring Defendants to implement and maintain reasonable security procedures, including, but not limited to: (1) ordering that Defendants utilize strong industry standard encryption algorithms for encryption keys that provide access to stored Sensitive Information; (2) ordering that Defendants implement the use of encryption keys in accordance with industry standards; (3) ordering that Defendants, consistent with industry standard practices, engage third party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests and audits on systems belong to Defendants and all others with whom they share Sensitive Information, on a periodic basis; (4) ordering that Defendants engage third-party security auditors and internal personnel, consistent with industry standard practices, to run automated security monitoring; (5) ordering that Defendants audit, test and train their security personnel regarding any new or modified procedures; (6) ordering that Defendants, consistent with industry standard practices, segment consumer data by, among other things,

creating firewalls and access controls so that if one area of Defendants' computer system is compromised, hackers cannot gain access to other portions of their systems; (7) ordering that Defendants purge, delete, destroy in a reasonable secure manner Sensitive Information no longer necessary; (8); ordering that Defendants, consistent with industry standard practices, conduct regular database scanning and security checks; (9) ordering that Defendants, consistent with industry standard practices, periodically conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and (10) ordering that Defendants implement industry best practices data security systems.

96. Plaintiffs further request that the Court require Defendants to identify and notify all members of the nationwide Class who have not yet been informed of the Data Breach.

97. Plaintiffs and the Class are entitled to actual damages in an amount to be determined at trial under Civil Code Section 1798.84.

98. Plaintiffs and the Class also are entitled to an award of attorney fees and costs under Civil Code Section 1798.84.

SEVENTH COUNT
Violation of the New Jersey Consumer Fraud Act, N.J.S.A. 56:8-1
(On behalf of Plaintiffs and the Nationwide Class)

99. Plaintiffs reallege and incorporate by reference each of the allegations set forth above.

100. Plaintiffs and all Class members are "consumers" as that term is defined by the New Jersey Consumer Fraud Act, N.J.S.A. 56:8-1.

101. Each Defendant is a "person" as that term is defined by the New Jersey Consumer Fraud Act, N.J.S.A. 56:8-1(d).

102. Defendants' conduct as alleged herein related to "sales," "offers for sale," or "bailment" as defined by N.J.S.A. 56:8-1.

103. Defendants advertised, offered, or sold goods or services in New Jersey and engaged in trade or commerce directly or indirectly affecting the citizens of the State of New Jersey.

104. One or more Defendants solicited Plaintiffs and Class Members to do business and uniformly and knowingly misrepresented to that by joining, their Sensitive Information was safe, confidential and protected from intrusion, hacking or theft.

105. Defendants misrepresented that they would protect the privacy and confidentiality of Plaintiffs' and Class Members' personal and confidential information, including by implementing and maintaining reasonable security measures.

106. Defendants intended to mislead Plaintiffs and Class Members and induce them to rely on their misrepresentations and omissions.

107. Defendants failed to implement and maintain reasonable security and privacy measures to protect Plaintiffs and Class Members' personal and confidential information in violation of N.J.S.A. 56:8-162, which was a direct and proximate cause of the Data Breach.

108. Defendants failed to provide notice to Plaintiffs and Class Members or otherwise comply with the notice requirements of N.J.S.A. 56:8-163.

109. Defendants' acts and omissions, as set forth herein, evidence a lack of good faith, honesty in fact and observance of fair dealing, so as to constitute unconscionable commercial practices, in violation of N.J.S.A. 56:8-2.

110. As a direct and proximate result of Defendants' unfair and deceptive acts and practices, Plaintiffs and Class Members are required to expend sums to protect and recover their

Sensitive Information, have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Sensitive Information, and thereby suffered ascertainable economic loss.

111. Plaintiff and Class Members seek all monetary and non-monetary relief allowed by law, including damages, disgorgement, injunctive relief, and attorneys' fees and costs.

EIGHTH COUNT
Violation of the Florida Deceptive and Unfair Trade Practices Act,
§ 501.201 et seq., Fla. Stat. ("FDUTPA")
(On behalf of Plaintiffs and the Nationwide Class)

112. Plaintiffs reallege and incorporate by reference each of the allegations set forth above.

113. Plaintiffs are "consumers" who used their credit cards to make payments to Quest. *See* § 501.203(7), Fla. Stat.

114. The FDUTPA prohibits "unfair methods of competition, unconscionable acts or practices, and unfair or deceptive acts or practices in the conduct of any trade or commerce." § 501.204, Fla. Stat.

115. Quest, by failing to inform consumers (including Plaintiffs and Class Members) of its unsecure, non-compliant, and otherwise insufficient data and information security practices, advertised, sold, serviced, and otherwise induced those consumers to purchase goods and services from Quest.

116. Quest knew or should have known that its computer systems and data security practices were inadequate to safeguard Plaintiffs' and Class Members' Sensitive Information, and that the risk of a data breach was highly likely.

117. Quest should have disclosed this information regarding its computer systems and data security practices because Quest was in a superior position to know the facts related to its defective data security.

118. Florida law requires notification of data breaches upon identification. Upon information and belief, Quest identified the Data Breach as early as March 2019, but only notified consumers on June 3, 2019, and therefore left those consumers at risk for the months in between discovery and notification.

119. Quest's failures constitute false and misleading representations, which have the capacity, tendency, and effect of deceiving or misleading consumers (including Plaintiffs and Class Members) regarding the security of its network and aggregation of Sensitive Information.

120. The representations upon which consumers (including Plaintiffs and Class Members) relied were material representations (*e.g.*, as to Quest's adequate protection of Sensitive Information), and consumers (including Plaintiffs and Class Members) relied on those representations to their detriment.

121. Quest employed these false representations to promote the sale of a consumer good or service, which Plaintiffs and Class Members purchased.

122. As a direct and proximate result of Quest's unconscionable, unfair, and deceptive acts or practices, Plaintiffs and Class Members have suffered and will continue to suffer injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and damages as prescribed by § 501.211(2), Fla. Stat., including attorneys' fees.

WHEREFORE, Plaintiffs and Class Members demand judgment as follows:

A. Certification of the action as a Class Action pursuant to Federal Rule of Civil Procedure 23, and appointment of Plaintiffs as Class Representatives and their counsel of record as Class Counsel;

B. That acts alleged herein be adjudged and decreed to constitute negligence and amount to violations of HIPAA, the California Customer Records Act, the California Confidential Medical Information Act, the California Unfair Competition Act, and the consumer protection laws of New York, California, New Jersey, and Florida;

C. A judgment against Defendants for the damages sustained by Plaintiffs and the Classes defined herein, and for any additional damages, penalties, and other monetary relief provided by applicable law;

D. By awarding Plaintiffs and Class Members pre-judgment and post-judgment interest as provided by law, and that such interest be awarded at the highest legal rate from and after the date of service of the Complaint in this action;

E. The costs of this suit, including reasonable attorney fees; and

F. Such other and further relief as the Court deems just and proper.

JURY TRIAL DEMANDED

Plaintiffs, individually and on behalf of all those similarly situated, hereby requests a jury trial, pursuant to Federal Rule of Civil Procedure 38, on any and all claims so triable.

Dated: June 6, 2019

Respectfully submitted,

/s/ Christopher A. Seeger

Christopher A. Seeger
Parvin Aminolroaya
SEGER WEISS LLP
55 Challenger Road
6th Floor
Ridgefield Park, NJ 07660

cseeger@seegerweiss.com
paminolroaya@seegerweiss.com

Jennifer Scullion (pro hac vice forthcoming)
SEEGER WEISS LLP
77 Water Street
8th Floor
New York, NY 10005
(212) 584-0700
jscullion@seegerweiss.com

Linda P. Nussbaum
Bart D. Cohen
NUSSBAUM LAW GROUP, P.C.
1211 Avenue of the Americas, 40th Floor
New York, NY 10036-8718
(917) 438-9189
lnussbaum@nussbaumpc.com
bcohen@nussbaumpc.com

Adam Frankel
GREENWICH LEGAL ASSOCIATES, LLC
881 Lake Avenue
Greenwich, CT 06831
(203) 622-6001
adam@grwlegal.com

*Counsel for Plaintiffs and the
Proposed Class*